PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-147072
(43)Date of publication of application : 06.06.1997

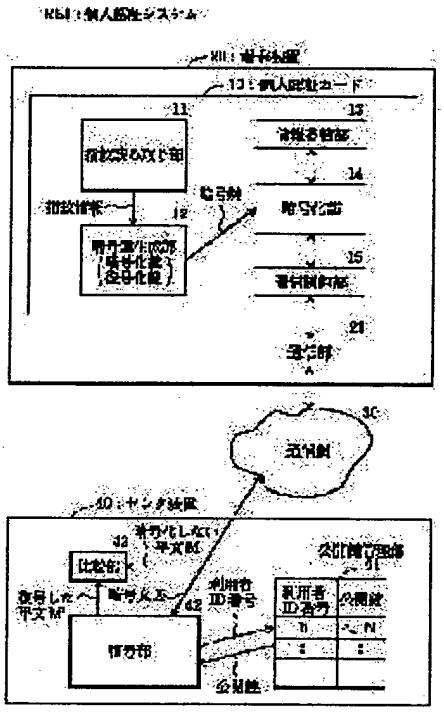
(51)Int.Cl. G06K 17/00
A61B 5/117
G06T 7/00
G06K 19/10

(21)Application number : 07-326467
(22)Date of filing : 21.11.1995

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : TAKANO MASAJI
GOMI KAZUHIRO
MATSUMURA TAKAHIRO
SUGIMURA TOSHIAKI

(54) PERSONAL AUTHENTICATION SYSTEM, PERSONAL AUTHENTICATION CARD AND CENTER EQUIPMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a personal authentication system, personal authentication card and center equipment with which such a trouble that a password number is necessary to be secretly memorized, can be excluded and there is no danger for fingerprint information from being stolen from the card and cables.
SOLUTION: A cryptographic key is generated 12 corresponding to the combination of read fingerprint information and the attribute of personal authentication card, prescribed information is enciphered 14 inside the personal authentication card by the enciphering key of this cryptographic key and the prescribed enciphered information, prescribed non-enciphered information and the ID of user corresponding to the read fingerprint are sent from terminal equipment to center equipment 40. On the other hand, the received prescribed enciphered information is deciphered 42 while using an open key corresponding to the ID of user received from terminal equipment 20, this prescribed deciphered information is compared with the received prescribed non-enciphered information and when both the information are equal to each other, it is judged that user is given personal authentication.



LEGAL STATUS

[Date of request for examination] 14.10.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－147072

(43)公開日　平成９年(1997)６月６日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ　17/00	Ｖ	
				Ｓ	
Ａ６１Ｂ　5/117		0277－2Ｊ	Ａ６１Ｂ　5/10	３２２	
Ｇ０６Ｔ　7/00			Ｇ０６Ｆ　15/62	４６０	
Ｇ０６Ｋ　19/10			Ｇ０６Ｋ　19/00	Ｓ	

審査請求　未請求　請求項の数７　ＦＤ　（全６頁）

(21)出願番号　特願平7－326467

(22)出願日　平成７年(1995)11月21日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　高野　正次
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　五味　和洋
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　松村　隆宏
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　川久保　新一

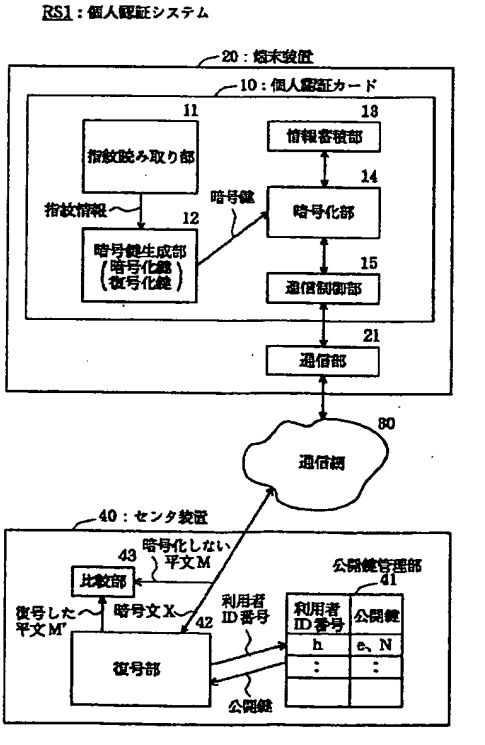
最終頁に続く

(54)【発明の名称】　個人認証システム、個人認証カードおよびセンタ装置

(57)【要約】

【課題】　暗証番号を秘密に記憶しておくという煩雑性を排除でき、また、指紋情報がカード、ケーブルから盗まれる心配がない個人認証システム、個人認証カードおよびセンタ装置を提供することを目的とするものである。

【解決手段】　読み取った指紋情報と個人認証カードの属性との組み合わせに応じて暗号鍵を生成し、この暗号鍵のうちの暗号化鍵によって、個人認証カード内で所定情報を暗号化し、暗号化された所定情報と暗号化されていない所定情報と読み取られた指紋に対応する利用者のＩＤとを端末装置がセンタ装置に送出し、一方、端末装置から受信した利用者のＩＤに対応した公開鍵を使用して、受信した暗号化所定情報を復号し、この復号された所定情報と受信した暗号化されていない所定情報とを比較し、両者が一致したときに個人認証されたと判断するものである。



1

【特許請求の範囲】

【請求項1】　指紋を読み取る指紋読み取り手段と；上記指紋の読取情報と個人認証カードの属性との組み合わせに応じた暗号鍵を生成する暗号鍵生成手段と；上記生成された暗号鍵のうちの暗号化鍵によって所定情報を暗号化する暗号化手段と；を個人認証カードが有し、

上記暗号化された所定情報と、暗号化されていない上記所定情報と、上記読み取られた指紋に対応する利用者のＩＤとを送出する信号送出手段を端末装置が有し、

各利用者に対応して公開鍵を記憶する公開鍵管理手段と；上記通信網から送信された上記利用者のＩＤに対応して上記公開鍵管理手段から読み出された上記公開鍵を使用することによって、上記通信網を介して送信された上記暗号化された所定情報を復号する復号手段と；この復号手段によって復号された所定情報と、上記通信網を介して送信された上記暗号化されていない所定情報とを比較し、両者が一致したときに個人認証されたと判断する比較手段と；をセンタ装置が有することを特徴とする個人認証システム。

【請求項2】　請求項1において、

上記個人認証カードの属性は、上記個人認証カード毎に異なるものであることを特徴とする個人認証システム。

【請求項3】　請求項1において、

上記暗号鍵生成手段は、

上記指紋の読取情報を所定の関数によって指紋特徴量に変換する指紋特徴量変換手段と；複数の素数を格納し、上記指紋特徴量変換手段が出力した指紋特徴量に応じた素数を、上記複数の素数から出力する素数格納手段と；を有するものであることを特徴とする個人認証システム。

【請求項4】　請求項1において、

上記個人認証カードは、上記指紋を読み取った時刻を上記センタ装置に送出し、上記センタ装置は、上記個人認証カードから送出された上記時刻と、上記比較手段が比較すべき時刻との差が所定の時間差を越えている場合には、個人認証されたと判断しないものであることを特徴とする個人認証システム。

【請求項5】　指紋を読み取る指紋読み取り手段と；上記指紋の読取情報と個人認証カードの属性との組み合わせに応じた暗号鍵を生成する暗号鍵生成手段と；上記生成された暗号鍵のうちの暗号化鍵によって所定情報を暗号化する暗号化手段と；上記個人認証カードの利用者のＩＤと、上記暗号化された所定情報と、暗号化されない所定情報とを送出する通信制御部と；を有することを特徴とする個人認証カード。

【請求項6】　請求項5において、

上記個人認識カードを開くと、上記個人認証カードの属性が消失するものであることを特徴とする個人認証カード。

【請求項7】　各利用者に対応して公開鍵を記憶する公開鍵管理手段と；暗号化された所定情報を復号化する復号化手段と；通信網から送信された利用者のＩＤに対応し、上記公開鍵管理手段から読み出された上記公開鍵を使用することによって、通信網を介して送信された暗号化された所定情報を復号する復号手段と；この復号手段によって復号された所定情報と、上記通信網を介して送信された暗号化されていない所定情報とを比較し、両者が一致したときに個人認証されたと判断する比較手段と；を有することを特徴とするセンタ装置。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、銀行のキャッシュサービス等のように、通信を利用した高度かつ重要なサービスを利用する際に、サービスセンタ等のセンタ装置への不正なアクセスを防止し、利用者個人の正当性を確認する認証技術に関するものである。

【０００２】

【従来の技術】銀行のキャッシュサービス等において、磁気カードやＩＣカード等によって個人を認証する場合、第1の従来方法では、そのカードが所有者本人に使用されていることを証明するために、利用者に暗証番号を入力させている。この場合、カードの所有者は、予め決められた暗証番号を記憶しておく必要があり、カードの所有者が暗証番号を記憶していなければならないという煩雑性がある。

【０００３】

【発明が解決しようとする課題】つまり、第1の従来方法では、正規の所有者のみが記憶しているパスワードのような秘密情報によって個人認証を行うので、個人認証カードの所有者に暗証番号を秘密に記憶させる必要があるという問題がある。

【０００４】この煩雑性を回避する方法として、暗証番号を使用する代わりに指紋を使用して、個人を認証する第2の従来方法が提案されている。

【０００５】この第2の従来例では、スキャナのような指紋を読み取る手段と、認証すべき利用者個人の指紋を予め記憶する手段と、読み取った指紋と記憶している指紋との一致を判断する手段とが設けられている。

【０００６】しかし、これらの手段が、センタ装置とは独立して設けられているので、各カードに記憶されている指紋情報が盗まれる危険性があるという問題がある。また、カードを使用する端末装置とセンタ装置との間で、ケーブル等を介して、上記指紋情報を交信する必要があり、上記指紋情報に関する秘密情報が、そのケーブルを介して、外部に漏洩する危険性があるという問題がある。

【０００７】本発明は、暗証番号を秘密に記憶しておくという煩雑性を排除でき、また、指紋情報がカード、ケーブルから盗まれる心配がない個人認証システム、個人認証カードおよびセンタ装置を提供することを目的とす

るものである。

【0008】

【課題を解決するための手段】本発明は、指紋を読み取る指紋読み取り手段と、指紋の読取情報と個人認証カードの属性との組み合わせに応じた暗号鍵を生成する暗号鍵生成手段と、生成された暗号鍵のうちの暗号化鍵によって所定情報を暗号化する暗号化手段とを個人認証カードに設け、暗号化された所定情報と、暗号化されていない上記所定情報と、読み取られた指紋に対応する利用者のＩＤとを端末装置が送出し、各利用者に対応して公開鍵を記憶する公開鍵管理手段と、通信網から送信された利用者のＩＤに対応して公開鍵管理手段から読み出された公開鍵を使用することによって、送信された暗号化された所定情報を復号する復号化手段と、この復号手段によって復号された所定情報と、上記通信網を介して送信された暗号化されていない所定情報とを比較し、両者が一致したときに個人認証されたと判断する比較手段とをセンタ装置に設けたものである。

【0009】

【発明の実施の形態および実施例】図１は、本発明の一実施例である個人認証システムＲＳ１を示すブロック図である。

【0010】個人認証システムＲＳ１は、個人認証カード１０と、端末装置２０と、通信網３０と、センタ装置４０とを有するものである。

【0011】個人認証カード１０は、指紋読み取り部１１と、暗号鍵生成部１２と、情報蓄積部１３と、暗号化部１４と、通信制御部１５とを有する。

【0012】指紋読み取り部１１は、利用者の指が押し当てられたときに、圧力等を微細に検出し、指紋の画像情報（指紋情報）を読み取るものである。

【0013】暗号鍵生成部１２は、個人認証カード１０の属性を有し、指紋読み取り部１１が読み取った指紋情報と個人認証カード１０の属性との組み合わせに応じた暗号鍵を生成するものである。なお、上記「暗号鍵」は、「暗号化鍵」と「復号化鍵」とを含むものである。また、上記実施例において、個人認証カード１０の属性は、図２に示すように、指紋特徴量変換部５０と素数表Ｔとによって抽出される素数である。

【0014】情報蓄積部１３は、通信文Ｍとしての所定情報（通信文Ｍには利用者のＩＤ番号が含まれる）を蓄積するものである。

【0015】暗号化部１４は、暗号鍵生成部１２によって生成された暗号鍵のうちの暗号化鍵によって所定情報を暗号化するものである。

【0016】通信制御部１５は、個人認証カード１０の利用者のＩＤと、上記暗号化された所定情報と、暗号化されない所定情報とを送出する通信制御部である。

【0017】端末装置２０は、通信網３０を介してセンタ装置４０と交信する通信部２１を有する。通信部２１

は、暗号化された所定情報と、暗号化されていない所定情報と、読み取られた指紋に対応する利用者のＩＤとをセンタ装置４０に送出するものである。なお、図１には、端末装置２０として通信部２１のみが記載されているが、他の機能をも有し、これらを省略して図示してある。

【0018】センタ装置４０は、公開鍵管理部４１と、復号部４２と、比較部４３とを有する。

【0019】公開鍵管理部４１は、各利用者に対応して公開鍵を記憶する手段である。復号部４２は、通信網３０から送信された利用者のＩＤに対応して公開鍵管理部４１から読み出された公開鍵を使用することによって、暗号化部１４で暗号化され、通信網３０を介して送信された所定情報を復号する手段である。段と；比較部４３は、復号部４２によって復号された所定情報と、通信網３０を介して送信され、暗号化されていない所定情報とを比較し、両者が一致したときに個人認証されたと判断する比較手段である。

【0020】図２は、個人認証システムＲＳ１における暗号鍵生成部１２を説明する図である。

【0021】暗号鍵生成部１２は、指紋の読取情報を関数Ｆによって指紋特徴量に変換する指紋特徴量変換部５０と、複数の素数ｐ、ｑ、ｕ、ｖ、ｗ、……を、上記指紋特徴量に対応して格納し、上記指紋特徴量変換手段が出力した指紋特徴量に応じた２つの素数ｐ、ｑを、上記複数の素数から出力する素数表（素数格納手段）とを有するものである。

【0022】なお、上記実施例において、暗号化の方式として、公開鍵暗号方式の１つであるＲＳＡ暗号方式を用いている。

【0023】次に、上記実施例における個人認証動作について説明する。

【0024】まず、利用者は、個人認証カード１０上の指紋読み取り部１１に指を押し当て、指紋情報を読み込ませる。この読み取られた指紋情報は暗号鍵生成部１２に送られ、指紋情報は関数Ｆによって指紋特徴量に変換され、この変換された指紋特徴量に応じて、素数表Ｔから２つの素数ｐ、ｑが出力される。なお、素数表Ｔには、たとえば５１桁の素数が焼き付けられ、素数表Ｔに格納されている素数またはその配列は、個人認証カード１０毎に異なっている。また、関数Ｆは、指紋読み取り部１１に指が当てられたときに、その当て方や圧力によって、関数値が変動しない頑強さを持つように作られている。

【0025】上記の場合、利用者毎に指紋情報が異なり、また、暗号鍵生成部１２における素数表Ｔの内容が個人識別カード１０毎に異なるので、暗号鍵生成部１２が出力する２つの素数ｐ、ｑは、結果的に、利用者と個人識別カード１０との組み合わせに応じてユニークに定まる。換言すれば、別の利用者が上記個人認証カード１

０を利用すると、別の素数の組み（たとえば、ｒとｓ）が選択される。

【００２６】そして、暗号鍵生成部１２から出力された素数ｐとｑとは、暗号化部１４に送られる。暗号化部１４において、素数ｐとｑとに応じて、ＲＳＡ暗号方式に必要な公開鍵ｅ、Ｎと、復号化鍵ｄとを、以下のようにして生成する。

【００２７】まず、

Ｎ：素数ｐとｑの積、

Ｌ：ｐ－１とｑ－１の最小公倍数、

ｅ：Ｌと素な数、

ｄ：Ｌ，ｅに対して１＝Ｌｃ＋ｅｄを満足する数である。

【００２８】つまり、（ｐ－１）と（ｑ－１）との最小公倍数Ｌを求め、この最小公倍数Ｌと素な数として公開鍵ｅを求め、また、ｐ×ｑ＝Ｎによって残りの公開鍵Ｎを求める。また、１＝Ｌｃ＋ｅｄを満足する復号鍵ｄを求める。この手順については、たとえば、「太田、黒澤、渡辺：情報セキュリティの科学．９５年．講談社．ｐｐ．１３３」に開示されている。

【００２９】なお、公開鍵ｅ、Ｎは、利用者ＩＤ番号に対応して、公開鍵管理部４１に保管されている。

【００３０】ところで、情報蓄積部１３には、センタ装置４０との間でやりとりされる通信文Ｍが蓄積されている。この通信文Ｍは、センタ装置４０との間で予め定められたフォーマットで蓄積され、たとえば、個人認証カード１０の製造番号（ＩＤ番号）、利用者の個人ＩＤ番号、カードリーダの製造番号（ＩＤ番号）、利用開始時刻等の情報が、上記通信文Ｍに含まれる。

【００３１】暗号化部１４では、暗号鍵生成部１２から暗号化鍵を受け取り、発信する通信文Ｍ（平文）を暗号文Ｘに変換する。この場合、

Ｘ＝Ｍ＾ｄ（ｍｏｄＮ）

の式を使用する。ここで、ｘ＾ｙは、ｘのｙ乗であり、ｚ（ｍｏｄｗ）は、ｚをｗで割った余りであり、ｄは、復号化鍵である。

【００３２】また、通信制御部１５は、端末装置２０の通信部２１を用いて、最適なプロトコルによって、暗号文Ｘと、通信文Ｍ（暗号文Ｘに対応する平文、利用者ＩＤを含む）とをセンタ装置４０に対して送信する。

【００３３】次に、センタ装置４０における利用者の認証動作について説明する。

【００３４】まず、復号部４２は、受信した通信文Ｍの中から、利用者ＩＤ、具体的には利用者ＩＤ番号ｈを抽出し、この抽出された利用者ＩＤ番号ｈに対応して公開鍵管理部４１に保管されている公開鍵ｅとＮとを公開鍵管理部４１から読み出す。そして、Ｍ’＝Ｘ＾ｅ（ｍｏｄＮ）の式に従って、センタ装置４０が受信した暗号文Ｘを平文Ｍ’に復号する。

【００３５】このようにして復号された平文Ｍ’と暗号化せずに受信した通信文Ｍとが一致するか否かを比較部４３が調べ、復号された平文Ｍ’と暗号化せずに受信した通信文Ｍとが一致すれば、その暗号文Ｘの発信者が正規の利用者であることを、センタ装置４０が認証する。

【００３６】ここで、第三者が、センタ装置４０から公開鍵ｅとＮと不正に盗み、さらに、個人認証させようとしたとする。しかし、ＲＳＡ暗号方式では、公開鍵ｅとＮとに基づいて、素数ｐ、ｑを導くことは、実効的にほぼ不可能であり、現在の計算機能力では、公開鍵ｅとＮとに基づいて素数ｐ、ｑを導くには、数百年以上かかるといわれている。上記実施例においては、素数ｐ、ｑ、ｄ等の素数の情報がなければ、平文Ｍから暗号文Ｘを導くことはできないので、個人認証に必要な暗号文Ｘを作ることができず、したがって、センタ装置４０における復号部４２で復号化する対象としての暗号文Ｘを復号部４２に送り込むことができず、不正に個人認証を行わせることができない。

【００３７】また、上記実施例において、端末装置２０からセンタ装置４０に送られる通信文Ｍの中には、個人認証カード１０によって個人認証を開始する時刻、つまり利用開始時刻の情報が含まれており、センタ装置４０において、その利用開始時刻と実際の時刻との差を演算し、この差の時間が所定時間を経過していれば、個人認証しないようにしてある。すなわち、正規の利用者が個人認証カード１０を使用して個人認証している間に、第三者が不正に、暗号鍵、通信文Ｍ等を盗用したとしても、その後に、その第三者が個人認証させようとした場合、その時刻が遅くなるので、個人認証がされず、安全性が高い。

【００３８】さらに、上記実施例において、不正な第三者が、個人認証カード１０を不正に入手し、正規の利用者になりすまして通信を開始しようとしたときには、指紋読み取り部１１が出力する指紋情報は、正規の利用者による指紋情報と異なるので、関数Ｆによって選ばれる素数の組みがｐ、ｑ以外のものになり、このような素数によって暗号化した暗号をセンタ装置４０においては復号できないので、誤って個人認証されることがない。

【００３９】ところで、上記実施例において、利用者の指紋情報そのものは、個人認証カード１０から外に出ず、また、個人認証カード１０内のどこにも記憶蓄積されないので、正規の利用者の指紋情報が第三者に盗まれることはない。また、利用者の指紋情報そのものをセンタ装置４０にも記憶していないので、この点からも、正規の利用者の指紋情報が第三者に盗まれることはない。

【００４０】さらに、個人認証カード１０自体を入手し、この個人認証カード１０のケースを開けて内部情報を見ることによって、素数ｐとｑや関数Ｆや素数表Ｔの中身を見破られる場合が考えられるが、この対策として、以下のようなことが考えられる。

①　素数表Ｔの内容を直接カードの外へは読み出せない

機構を個人認証カード１０に付加する。

② 個人認証カード１０が開けられた場合には、個人認証カード１０内に記憶されている情報が全て消失する構成を採用する。

③ 素数表Ｔ上の素数のエントリ数を多くすることによって、正しい素数の組みｐとｑが発見される確率を低くし、これによって、正しい素数の組みｐとｑが発見されることを実効的に困難にする。

【００４１】また、上記実施例において、暗号鍵生成部１２が出力する情報は、指紋情報と個人認証カード１０とによって割り当てられた適当な素数であり、これは暗号化のための情報に過ぎない。したがって、素数がたとえ盗聴され解読されたとしても、指紋情報そのものは不正な第三者に盗まれることがない。上記実施例においては、実際には、センタ装置４０の保守者や個人認証カード１０の所有者自身も、自分の指紋情報そのものを知り得ない。

【００４２】なお、上記実施例において、暗号鍵生成部１２における素数表Ｔの内容が、どの個人識別カード１０においても同じであるようにしても、上記と同様の動作を行う。

【００４３】

【発明の効果】本発明によれば、個人の認証に必要な秘密情報である指紋情報そのものは、個人認証カードの外部には出ず、また、個人認証カード内のどこにも記憶蓄積されないので、重大な問題となりうる個人の指紋情報そのものが漏洩される危険性がないという効果を奏する。

【図面の簡単な説明】

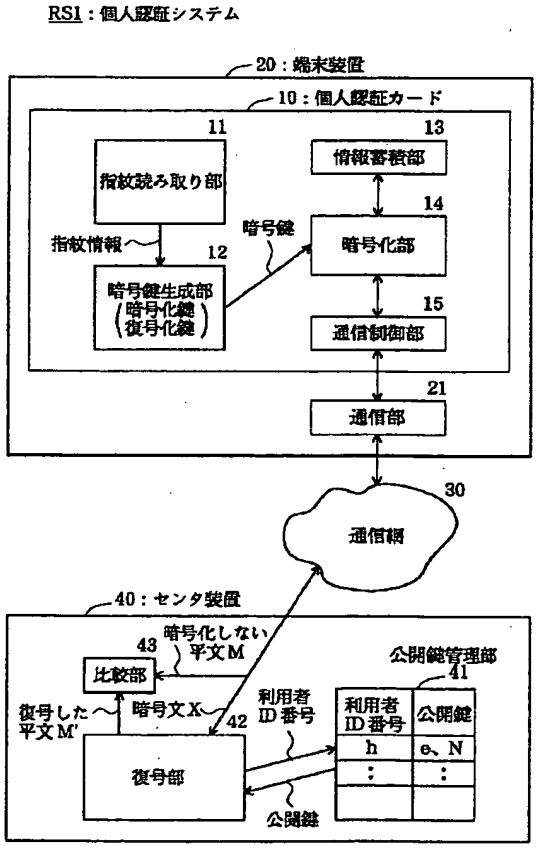
【図１】本発明の一実施例である個人認証システムＲＳ１を示すブロック図である。

【図２】個人認証システムＲＳ１における暗号鍵生成部１２を説明する図である。

【符号の説明】

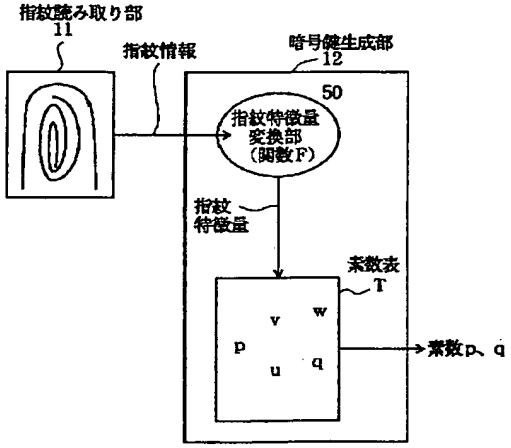
１０…個人認証カード、
１１…指紋読み取り部、
１２…暗号鍵生成部、
１３…情報蓄積部、
１４…暗号化部、
２０…端末装置、
４０…センタ装置、
５０…指紋特徴量変換部、
Ｔ…素数表。

【図１】



K3688

【図２】



K3688

フロントページの続き

(72)発明者　杉村　利明
東京都新宿区西新宿三丁目19番２号　日本
電信電話株式会社内